科学论文发表中的信息安全问题及对策——基于多主体视角

段尧清　郑卓闻[1]　王蕊

湖北省数据治理与智能决策研究中心，华中师范大学信息管理学院
湖北省武汉市洪山区雄楚大道382号华中师范大学南湖校区,430079

摘　要：［目的］分析科学论文发表中信息安全的现状及存在问题，有利于提升我们对我国总体国家安全观的理解，明确该领域未来的发展方向；［方法］基于全生命周期理论，从多主体视角对科学论文发表中信息安全问题进行规范分析与理论构建；［结果］构建了科学论文发表中各贡献主体信息安全生态体系，提出了多主体视角下科学论文发表中信息安全的五维一体提升路径；［结论］科学论文发表中信息安全问题是需要正确认识和把握的重大理论和实践问题之一，是在新的外部环境、新的技术革命和新的竞争格局下的一个全新课题，同时呼唤新的认识论和方法论来深化对该问题的认识。

关键词：　科学论文发表；信息安全；问题与对策；提升路径
DOI：

1 引言

随着人工智能、大数据、云计算、数据挖掘和区块链等技术的快速发展，各个领域的数字化转型进入了常态化阶段，我国正逐步从工业社会过渡到信息化社会。由此产生的大量业务信息在互联网中流通，这些信息真实反映了客观世界的运行情况，蕴含了大量的社会和经济价值，如果被不法分子滥用和盗用，轻则损坏个人财产和生命安全，重则危害社会和国家安全。习近平总书记在2014年首次提出了十二种总体国家安全观，将信息安全视为其中重要的一种。党的十九大报告中同样强调，要同时重视传统安全和非传统安全两种，其中信息安全便属于非传统安全。为了规范互联网信息的使用规范和保障信息安全，我国自2015年以来出台了多项政策法规，如2015年出台了《国家安全法》、2017年出台了《网络安全法》、2019年出台了《中华人民共和国密码法》、2021年出台了《数据安全法》以及同年出台了《个人信息保护法》。此外，还出台了《关键信息基础设施安全保护条例》《网络数据安全管理条例》和《信息安全技术个人信息安全规范》等多套行业标准，这些政策法规和行业标准的完善标志着我国信息安全治理的法制框架的形成，我国逐渐迈入信息安全法治化监管阶段。

然而，在科学论文发表这一领域，我国仍然面临诸多现实问题，科学论文发表中信息安全事件频发。在论文发表过程中，大量有关作者本身、论文内容、创意创新和研究方法的关键信息被泄露，严重损坏了作者的个人知识产权。一些公开发表的论文，其研究发现和结论通常是基于收集和分析大量准确的事实数据，而这些所采集到的事实数据，反应我国现实发展的实际情况，如果论文忽略对国家安全的考量，将会对国家安全和社会稳定造成严重不良影响。对于科研机构和出版社而言，其外部信息安全威胁正随着技术的飞速发展而不断升级，业务数据化、系统数字化、信息网络化等众多因素增加了科研机构内部信息面临的泄露风险。机构外部势力通过攻击信息系统漏洞、化解防护等技术手段，实施科学论文信息的窃取、篡改和非法使用等活动，机构内部的部分管理人员利用特权和职务之便，可以轻而易举的获取尚未发表的论文的关键信息，进而导致信息泄露、破坏和丢失等情形。由于信息的潜在经济价值被进一步认识，由此带来的暗网中寻求非法信息交易的活动也愈加频繁，机构内外部势力所泄露的数据会在暗网中更迅速的传播，非法窃取者也将会获取更高额的汇报，这进一步增加了科学论文信息安全问题带来的国家安全风险。

学界目前关于信息安全技术应用的研究成果丰富，主要通过探讨区块链[1-2]、深度学习[3]等技术在大数据[4-5]、云计算[6-7]、物联网[8-9]等环境下对信息安全的适配性，逐步构建了一定的信息安全保护架构。同时，

[1] 通讯作者：郑卓闻，574144157@qq.com

学者们对金融[10]、医疗[11]、工业[12]等众多领域的网络信息安全保护策略[13-14]、信息安全素养[15]、网络信息安全影响因素[16-18]等内容也进行了深刻的讨论。虽然当前在科学论文发表领域的研究明显不足，但在信息安全领域丰富的理论成果和实践成果，能够为科学论文发表领域的信息安全理论构建提供足够研究基础。

2 科学论文的分类与发表中信息安全定义

2.1 科学论文的分类

论文分类标准依据不同的分类标准有不同的分类类型，科学论文可以被分为六种，按照学科类型划分，可以分为社会科学学术论文和自然科学学术论文；按照学科性质划分，可以分为基础学科学术论文和技术应用学科学术论文；按论证方式划分，可以分为基础理论型、方法技术型、调查报告型、文献综述型、应用研究型和学术争论型学术论文；按写作内容划分，可以分为专题型学术论文和综合型学术论文；按研究范围划分，可以分为宏观研究学术论文和微观研究学术论文[16]；按国家《科学技术报告、学术论文和学术论文编写格式》划分，可以分为期刊论文和学位论文。不同类型的科学论文在发表中存在差异性的信息安全问题，比如学位论文常存在学术不端现象，初学者的学科理论知识不足，常会在撰写论文中有意无意的使用他人的核心研究成果，如果处理不当会侵犯其他作者的知识产权。另外学位论文常常会被作者拿到临近打印店进行纸质版打印以及使用网络上廉价的第三方查重服务，这些行为会极大增加论文外泄风险。期刊论文的发表流程有别于学位论文，作者向杂志投稿后一般由审稿人和编辑协助完成后续论文的发表工作，虽然也会出现上述信息安全问题，但更多的是会出现尚未发表的论文被特权人员非法泄露或在论文传输和存储过程中被机构外部势力非法入侵系统获取等情形。具体如表1所示。

表1 科学论文的分类

按学科类型划分	社会科学学术论文
	自然科学学术论文
按学科性质划分	基础学科学术论文
	技术应用学科学术论文
按论证方式划分	基础理论型
	方法技术型
	调查报告型
	文献综述型
	应用研究型
	学术争论型
按写作内容划分	专题型学术论文
	综合型学术论文
按研究范围划分	宏观研究论文
	微观研究论文
按国家《科学技术报告、学术论文和学术论文编写格式》划分	期刊论文
	学位论文

2.2 科学论文发表的定义及生命周期

依据《中华人民共和国数据安全法》和《中华人民共和国网络安全法》中对数据安全、网络安全和个人信息安全的定义，本文定义科学论文发表中的信息安全是：采取必要的法律、技术和管理手段，防范对科学论文发表系统的攻击、侵入、干扰、破坏和非法使用以及意外事故，保证科学论文在发表各个阶段中涉及到的各类型信息处于被合法合规采集和利用的安全状态，以及保障持续安全状态的能力。

科学论文从内容结构上一般可以分为七部分：研究主题、研究问题、文献回顾、研究设计、研究实践（调查研究与实证类）、研究发现与研究结论。在科学论文的不同部分，信息安全问题也有差异。例如，在

研究主题方面多存在创意创新和选题方向的学术剽窃问题，在研究实践方面，所使用的数据可能来源于他人研究或有泄露国家秘密的风险等。

科学论文发表的一般过程大致为：选题、构思、撰写、送审、返修、查重、发表/拒稿。如果被拒稿则会重新开始新的生命周期，如图1所示。生命周期中的每一个环节，都存在不同情形的信息安全隐患。比如论文在选题和构思中盗用或抄袭了他人创意，撰写中抄袭他人的语句或有意无意的泄露国家机密，送审和返修往往会通过在线信息系统，在多接口 API 的传输中除了会面临被黑客攻击的风险意外，还可能会被机构内部人员主动外泄等。因此，有必要在科学论文发表的业务实践中要厘清各环节可能出现的信息安全问题。

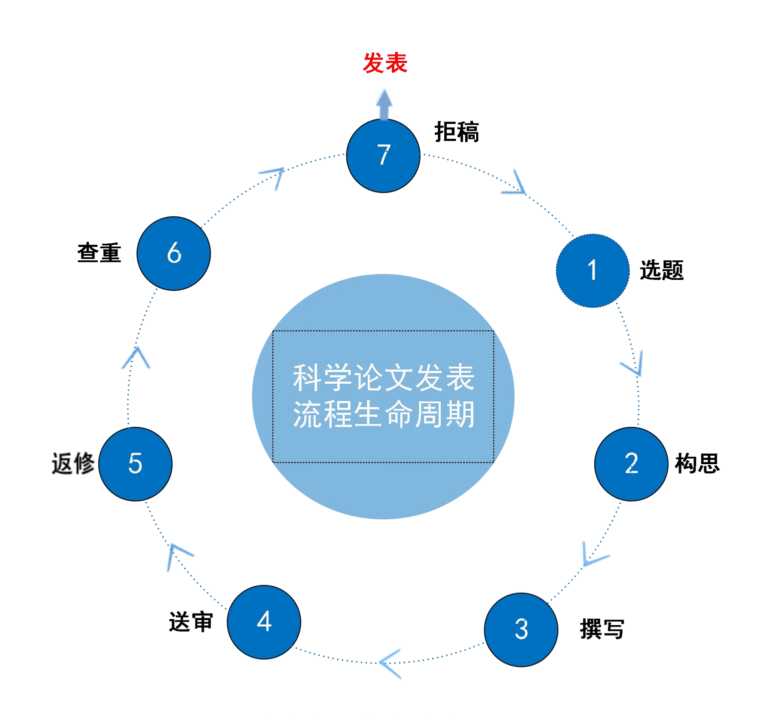


图1 科学论文发表生命周期

2.3 科学论文的发表中各贡献主体的信息安全生态体系构建

一篇科学论文的成功发表，往往是多个主体共同努力的结果。本文构建了科学论文发表中各贡献主体信息安全的生态体系，厘清了三个主要贡献主体（作者、审稿人、编辑）在论文发表过程中，与其它主体在交互时可能会产生信息安全的问题。此外，还基于多主体视角总结了科学论文发表中信息安全的类型，分别是：个人信息安全、课题组信息安全、机构信息安全、行业领域信息安全和国家信息安全。

如图2所示，作者、编辑与审稿人这三个主要贡献主体相互独立又关系密切，而个人、课题组、机构、行业领域和国家又代表了在科学论文发表过程中可能会产生信息安全问题的主体。例如，科学论文的作者可能会有意无意的对其它论文的作者、课题组、科研机构、行业领域带来有关信息安全方面的影响，更严重者可能会影响国家安全。同样的，审稿人和编辑作者出版社的机构内部成员，能够访问一般作者无法访问的科学论文数据库，同样可能会对其它作者（个人）、课题组、机构、行业领域和国家信息安全带来影响。

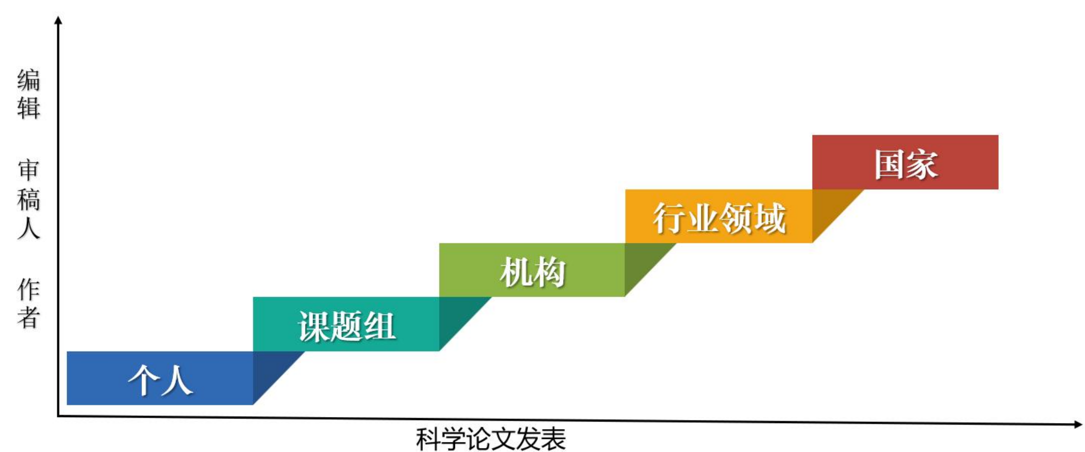


图2 科学论文发各贡献主体生态体系

3 科学论文发表中信息安全存在的问题

科学论文发表的根本目的是促进学术交流与知识共享，促进科学成果的累计，推动整个科学领域更快速发展。因此，科学论文发表的本质是开放共享，科研成果应该无差别的向全社会所有有需要的科研工作者公开，促进学术交流的同时将自己的学术贡献积累到整个科研领域中，以便后续科研工作者能够在此基础上进行更深层次的探索。但信息安全却强调限制开放、保密、增加共享条件等，这与科学论文发表的本质貌似是相违背的。科学论文的一些敏感信息是需要被保密的，不能完全公开，即便公开也要被认定为作者的知识产权，不能随意的被他人使用，比如尚未公开发表论文的研究内容、研究方法、数据、创意等信息，一旦在发表前被泄露，会严重损害作者个人权益，并逐渐降低各领域作者对原创的追求热情。还有一些涉及当前国家机密的信息，也不能被完全公开。比如国家前沿科技发展的信息、国家最新军事动态的信息、重大突发事件发展的关键信息等，这些信息一旦不加以甄别向全社会开放，会成为不法分子和国内外反动势力危害国家安全和社会稳定的工具。由此产生了科学论文发表中信息安全问题的两大矛盾点：开放与涉密、知识共享与知识产权。如何既在保证涉密信息安全不被公开，保障多元主体的信息安全的前提下，最大限度的深化科学论文信息共享开放，提升知识循环流动效率，是亟待解决的矛盾点，也是未来重点研究方向之一。在这样两组矛盾点的前提下，当前我国科学论文发表中信息安全产生了一些痛点问题，具体如下。

（1）作者个人信息安全意识薄弱

不少科学论文作者对信息安全保护得意识不足，常会有意无意地泄露个人信息或侵犯他人的信息安全。很多初入学术领域的研究人员仍然在具有商业性质的打印店进行论文打印，为了追求廉价还会在网上寻求不正规得第三方机构进行论文查重检验等。作者这些无意识的主动泄露行为，再配上第三方机构有获取非法利益得动机，很容易造成科学论文在尚未发表前就被泄露。此外，还有一些作者在个人论文中剽窃、盗用和篡改他人研究成果，构成了学术不端的行为，也危害了其他作者的科学论文信息安全。在国家机密方面，由于缺乏政治敏感性，一些作者将涉及国家安全的机密性文件和信息写入论文并公开发表，这种行为很容易被国内外反动势力团体利用，提升了国家安全面临的风险。

（2）特权人员信息泄密风险较大

特权人员在这里主要指科研机构的工作人员、审稿人和编辑等，他们通常在科学论文的发表中管理者某些事务，能够通过职务之便在信息系统中获取到敏感信息。如国家科研机构内部的一些管理人员，可以掌握到我国相关涉密科技发展的最新动态，并利用其掌握的最新信息进行论文创作，危害国家安全。1999年我国出现了歼十战机的机密参数信息在论文中被泄露的案例，泄露者正是我国某研究所的助理工程师。还有一些杂志、科研机构的编辑和审稿人，可以获取尚未发表的论文与尚未被审批的项目申报书，进而对其进行抄袭、篡改和出售等行为，对投稿人的知识产权造成严重破坏。综合来看，特权人员可以轻易获取关键信息，但机构对他们的管理却相对松散，信息安全泄露事件频频发生。

（3）技术进步提升安全监管难度

目前计算机和大数据分析技术日益成熟，机构运行也都经历了数字化转型，科学论文发表中几乎所有的业务都可以通过互联网和信息系统完成，这为科研人员在网络中获取和利用数据提供更为便捷的方式，也极大提升了论文发表效率。但互联网技术的不断成熟也意味着科研人员可以通过网络更轻易地获取他人研究成果等其它有价值的论文信息，对他人的选题、构想、方法、创意和数据等直接据为己用。还有些作者在收集有关国计民生数据的时候，利用先进的爬虫技术对互联网中的社交媒体平台、各组织机构网站和政府网站的涉密数据库等进行深度数据爬取，采取了违法违规的手段获取有关用户个人和国家安全的隐私信息。虽然各大互联网平台也不断地更新反爬虫技术手段，但依然会有一些不法分子越过防盗技术，成功爬取相关涉密信息。互联网交互中的匿名性，会帮助不法分子更好的隐藏自己的身份，而强大的数据分析工具（爬虫技术、数据挖掘技术、数据脱敏技术等）也会帮助他们以更低廉的成本开展违法违规的窃取活动。

从科研管理信息系统的使用角度方面来看，目前的业务系统通常是手机、台式电脑、笔记本电脑、平板电脑等设备共同使用，这种多元互通的业务操作系统为科学论文发表提供了便捷，但由于各种设备本身的系统架构和技术有差异，使得其面临着承受更多形态外部黑客攻击的风险。此外，目前除了将科学论文存储在本地实体硬盘中，更多作者还会选择将论文和数据等关键信息存储在云端硬盘，这也进一步加剧了相关信息泄露的风险。此外，科学论文发表系统通常具有多个 API 接口，比如电子邮箱和查重服务接口等，论文在通过 API 接口传输时，也会成为外部黑客攻击系统，获取科学论文数据的重要途径。整体上来看，技术的进步在给科学论文发表带来便利的同时，也不断涌现出新的危害信息安全的方式。

（4）行业政策标准缺失

数据安全领域出台了诸多法律法规，如《网络安全法》《个人信息保护法》《数据安全法》《网络数据安全管理条例（征求意见稿）》等。但在科学论文发表领域，尚缺乏体系化、专业化、统一化的政策标准。相较于众多综合性的信息安全保护法规与行业标准，目前仅有2016年颁布的《涉密研究生与涉密学位论文管理办法》与2018年颁布的《科学数据管理办法》等少量政策文件是国家出台的科学论文发表领域行业专属政策法规，对标金融和工业领域已经构成了完善的政策法规体系和行业指导标准，本领域在政策标准方面的重视程度还远远不够。

4 科学论文发表中信息安全的对策与建议

针对上述痛点问题，提出了多主体视角下科学论文发表中信息安全的五维一体提升路径，如图3。其中，认知是前提，法律是保障，技术和管理是手段，业务是实践的主要阵地。

（1）认知维

作者、课题组和机构首先需要意识到科学论文发表中信息安全保护的重要性，还应全面学习和深刻掌握信息安全的表现形式、可能会造成信息安全问题的行为和主要规避方法。通过组织开展讲座论坛和专题课程等形式对作者进行科学论文发表中信息安全问题的持续培训，提升其信息安全素养。行业领域和国家则需要重视这一领域的发展和研究，厘清科学论文发表中信息安全的主要矛盾、相关利益主体和未来发展方向等相关问题，只有意识到这些问题的内涵和重要性，才能更好的制定政策标准，引入相关技术和管理手段，引导业界学者开展这一方面的学术研究，指导业务实践。

（2）法律维

利用法律法规和政策标准来引导和保障科学论文发表中信息安全治理活动的有序开展。以目前国家已出台的数据安全法律法规和行业标准为基础，并参考金融领域和工业领域等发展较为成熟和领先的行业中有关信息安全法律法规和标准，构建从科学论文发表中的信息安全标准到信息安全等级评估到管理办法等的内容完备的法律保障体系，完善法治化顶层架构设计，确保个人、课题组、机构和行业有法可依，有标准可执行。

（3）技术维

国家、行业和机构应积极引入新信息技术，开发统一的论文发表平台，最大限度促地进论文信息协同

共享，同时提升机器自动处理效率，减少作者、审稿人和编辑的人工干预，降低泄密风险。利用联邦学习，解决不开放情境下科学论文发表过程中信息协同与融合问题，在保证信息安全的前体下，推动信息在各平台加速流通，实现信息跨平台、跨业务和跨层级融合。既保护了知识产权，又能够推动知识交换效率，妥善解决“开放与涉密”和“知识共享与知识产权”等矛盾。还可以借鉴区块链加密技术中身份链、数据证明、智能合约等核心思想，针对科研论文发表中各环节中信息的创建、融合和交换等不同阶段，围绕作者、审稿人、编辑和平台等不同主体，建立科学论文发表中信息所有权、使用权和收益权的保护模式，同时为了避免链上信息被使用者滥用，还可以建立一种基于信息证明的使用权授予机制，保证只有在创作者者和管理者许可的情形下信息才能被访问使用。还可积极引入人工智能与自然语言识别技术，进一步提升机器对科学论文文字自动识别的准确度，除了常规的词组与语句剽窃识别外，对科学论文的创意、数据来源、研究方法等不易识别却又异常关键的部分进行更有效地查重，更加灵敏、准确地感知和识别到一些作者通过使用数据脱敏等技术，使其剽窃内容能够躲避机器查重的相关内容。

（4）管理维

目前科研工作有信息化程度高、泄密隐患大、技术手段更新快、科研场所更加灵活、科研参与人员多、涉及人员成分复杂、新进科研人员频率高等特点，应有针对性的定期开展诸如培训、宣传、问责、审查等管理手段，加强科研人员信息安全意识与能力。各科研机构应制定适合自身的科研论文发表道德规范与管理办法，并设立专职专人对审稿人、编辑、投稿系统等开展监管工作，明确权责界限，制定相互监督和制约的工作机制，杜绝机构内部的特权人员利用职务之便非法获取科学论文的相关信息。同时也应对科学论文发表信息系统进行定期的安全筛查，及时识别来自系统外部的攻击并采取相应的止损所示，重点人员的计算机、帐户、邮箱和硬盘等也应定期进行病毒查杀，以降低来自系统外部的攻击风险。

（5）业务维

科学论文发表中的业务实践是认识前提、法律保障、技术和管理手段综合应用产生的结果，同时又反过来影响其它四维。行业领域和各科研机构需要在业务实践中认识到其它四维给业务带来的影响，通过提供法制化、流程化和标准化的政策体系为保障完善顶层设计，利用区块链、联邦学习和人工智能等技术为载体构建统一的科学论文发表管理平台，开展定期审查和问责活动为管理手段约束相关特权主体过度使用其权限，来保护投稿作者的知识产权。同时，在业务实践中，又需要收集大量来自作者、课题组、科研机构和行业领域的反馈信息，这些信息能够反应不同主体在业务实践中的实际需求，评价正在施行的政策法规、技术和管理手段的运行效果，有利于下个阶段的提升与优化。五维一体的提升路径体系形成了良性发展的循环态势，五个维度相互影响相互补充，稳步提升科学论文发表中的信息安全。

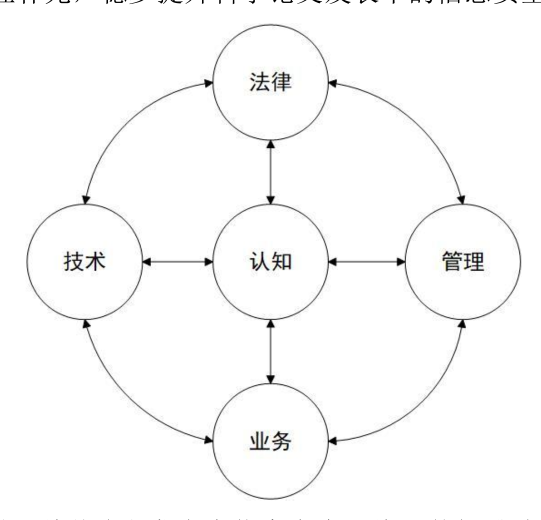


图3 科学论文发表中信息安全五维一体提升路径

5 总结

本文对科学论文的分类、结构、发表的生命周期、定义等问题进行了讨论，构建了多主体视角下科学

论文发表中各贡献主体的信息安全生态体系，并总结了不同主体在科学论文发表中所面临的不同类型的信息安全问题。本文认为科学论文发表中信息安全有三点认识：第一，科学论文发表信息安全是需要正确认识和把握的信息安全的重大理论和实践问题之一；第二，是一个全新的课题，具体表现在：新的外部环境、新的技术革命和新的竞争格局带来的新问题；第三，呼唤新的认识论和方法论来深化对这一问题的解释，如论文发表的价值取向、底线思维、平衡思维等。

参考文献：

[1]刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展[J].软件学报,2018,29(07):2092-2115.

[2]吴振铨,梁宇辉,康嘉文,余荣,何昭水.基于联盟区块链的智能电网数据安全存储与共享系统[J].计算机应用,2017,37(10):2742-2747.

[3]孙浩,陈进,雷琳,计科峰,匡纲要.深度卷积神经网络图像识别模型对抗鲁棒性技术综述[J].雷达学报,2021,10(04):571-594.

[4]王世伟.论大数据时代信息安全的新特点与新要求[J].图书情报工作,2016,60(06):5-14.

[5]张茂月.大数据时代公民个人信息数据面临的风险及应对[J].情报理论与实践,2015,38(06):57-61+70.

[6]薛燕,朱学芳.基于改进加密算法的云计算用户隐私保护研究[J].情报科学,2016,34(09):145-149.

[7]仇蓉蓉,胡昌平.云计算环境下国家数字学术资源信息安全协同治理框架研究——基于信息生态视角[J].图书情报工作,2022,66(08):55-62.

[8]吴武飞,李仁发,曾刚,谢勇,谢国琪.智能网联车网络安全研究综述[J].通信学报,2020,41(06):161-174.

[9]宋涛,李秀华,李辉,文俊浩,熊庆宇,陈杰.大数据时代下车联网安全加密认证技术研究综述[J].计算机科学,2022,49(04):340-353.

[10]靳玉红.大数据环境下互联网金融信息安全防范与保障体系研究[J].情报科学,2018,36(12):134-138.

[11]李洪晨,马捷,胡漠.面向健康医疗大数据安全保护的医疗区块链模型构建[J].图书情报工作,2021,65(02):37-44.

[12]靳江红,莫昌瑜,李刚.工业控制系统功能安全与信息安全一体化防护措施研究[J].工业安全与环保,2020,46(01):53-60.

[13]冷晓彦.大数据时代的信息安全策略研究[J].情报科学,2019,37(12):105-109.

[14]张艳丰,王羽西,邹凯,彭丽徽.基于模糊DANP的智慧城市信息安全风险要素识别与管理策略研究[J].情报理论与实践,2020,43(10):144-150.

[15]陈琦,熊回香,代沁泉,顾佳云.平台社会视阈下大学生网络信息安全素养能力评价及提升策略研究[J].图书情报工作,2022,66(07):75-87.

[16]王晰巍,王雷,贾若男,王铎.社交网络中个人信息安全行为影响因素的实证研究[J].图书情报工作,2018,62(18):24-33.

[17]邹凯,向尚,张中青扬,毛太田.智慧城市信息安全风险评估模型构建与实证研究[J].图书情报工作,2016,60(07):19-24.

[18]周凤飞,王佳佳.大学生智能手机用户信息安全意识与行为调查分析[J].图书情报工作,2018,62(10):47-53.

[19]姚先国等.经济类学生毕业论文写作指导[M]. 杭州：浙江大学出版社，2004：4.

Information Security Issues and Countermeasures in Scientific Paper Publishing - Based on a Multi-subject Perspective

Abstract

[Purposes] Analyzing the current situation and problems of information security in the publication of scientific papers is conducive to enhancing our understanding of China's overall national security concept and clarifying the future direction of development in this field;

[Methods] A normative analysis and theoretical construction of information security in the publication of scientific papers from a multi-subject perspective based on the whole life cycle theory;

[Findings] The ecological system of information security for each contributing body in scientific paper publication is constructed, and the five-dimensional path of improving information security in scientific paper publication from the perspective of multiple bodies is proposed;

[Conclusions] The issue of information security in the publication of scientific papers is one of the major theoretical and practical issues that need to be properly understood and grasped, and is a brand new topic under the new external environment, the new technological revolution and the new competitive landscape, while calling for a new epistemology and methodology to deepen the understanding of the issue.

Keyword Scientific paper publication; Information security; Problems and countermeasures; Improvement path

[作者贡献声明]：作者 1：提出科学论文发各贡献主体生态体系、多主体视角下科学论文发表中信息安全的五维一体提升路径，提出研究方向，设计论文框架，参与论文修订；

作者 2：文献调研与整理、撰写论文；

作者 3：进行对比实验，数据采集与分析数据，修订论文。

。